Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 235 (2024) 1649–1663

Procedia Computer Science

www.elsevier.com/locate/procedia

International Conference on Machine Learning and Data Engineering (ICMLDE 2023)

A Critical Review on Cybersecurity Awareness Frameworks and Training Models

Hamed Taherdoost [a,*]

[a] *Westcliff University, Irvine, USA*

Abstract

Due to its inherent weaknesses, protecting data and maintaining its integrity is crucial in the changing world of cybersecurity. This evaluation employs a quantitative methodology to evaluate several cybersecurity awareness and training approaches to illuminate their efficacy in lowering costs and security incidents for a company while enhancing cyber resilience and security posture. Our thorough research, which is supported by actual evidence, emphasizes the real advantages of clear cybersecurity awareness and training activities. These measures enable businesses to drastically reduce security incidents and realize verifiable cost reductions. Additionally, these initiatives act as accelerators for improving overall cyber resilience, therefore bolstering an organization's security posture. This in-depth analysis offers a data-driven perspective on these models' respective capabilities and highlights the critical role that strategic cybersecurity education and awareness play in defending against a constantly changing threat environment.

Keywords: **Cybersecurity; Awareness; Frameworks; Education and Training; SecurityLifecycle**

1. Introduction

Over the past decade, advancements in Information Technology have led to widespread use of the Internet across all spheres of society, from schools and govern-ments to corporations and industries [1, 2]. When using the internet for extended pe-riods, users of any age face several potential security threats. A company can lose data, customers, or

* Corresponding author. Tel.: +1-236-889-5359
E-mail address: hamed.taherdoost@gmail.com

1877-0509
10.1016/j.procs.2024.04.156

its reputation even if it employs the best cyber security measures [3]. Cybersecurity is a technological issue that is exacerbated by non-expert end users who interact with internet content [4].

Despite this, many netizens are still not sufficiently aware of the numerous inter-net threats. This is even though internet consumption is rising drastically as a result of information technology advancements [5]. They frequently lack the fundamental skills needed to secure their computing equipment. The worst-case scenario is that individu-als are totally oblivious to the dangers posed by cyberspace. Consequently, they are unprepared to implement defensive cybersecurity measures. Due to the complexity and constant evolution of security, technological defenses alone are rarely adequate to protect these individuals from online threats. Individuals are responsible for modify-ing their privacy settings, adhering to security policies, and selecting secure passwords. These judgments require informed decision-making, foresight, and tradeoffs based on users' current awareness of online dangers and the technologies they use [6-8]. There-fore, enhancing the awareness and knowledge of non-expert end users is a crucial step toward cybersecurity.

The term "cybersecurity awareness" refers to "an approach to train internet users to be sensitive to the different kinds of cyberattacks and the vulnerability of data and computers to these threats" [9]. According to a study by Shaw et al. [10], cybersecurity awareness is "the extent to which users are aware of the importance of information security and their obligations to exercise adequate information control levels to safe-guard the organization's data and networks". So, warning internet users about cyber-security risks and improving their comprehension of those risks are two main objec-tives of cybersecurity awareness. Hence, they will embrace security while using the in-ternet. As a result, strengthening security at both the personal and organizational lev-els requires minimizing human-related mistakes or vulnerabilities [11].

Companies should regularly teach all staff in cybersecurity awareness to prevent or minimize the impact of cyberattacks on business performance and, consequently, the infringement of intellectual property and organizational knowledge [12]. Users in cybersecurity education and awareness programs are made aware of the company's policies, rules, and regulations as well as the security measures that need to be done to secure sensitive data. Staff can practice and consistently apply this information to de-velop the cyber-security skills necessary to effectively track and respond to cybersecu-rity hazards and threats [13].

Adequate staff training regarding secure online behavior and security counter-measures remains the cornerstone of businesses' cybersecurity strategies as security events continue to increase in frequency, sophistication, and expense. Better security training for staff is suggested to be the optimal cybersecurity investment by Disparte and Furlow [14]. Because of this, businesses need to spend money on cybersecurity awareness training to increase staff readiness and knowledge [12]. Although this is the case, cybersecurity awareness training projects frequently lack funding [15]. In addi-tion, a lot of employees disregard the information security guidelines set forth by their employers [16]. This noncompliance raises concerns about the efficiency of many cybersecurity awareness training projects while also increasing the risk of security and data breaches [17]. Consequently, an effective cybersecurity awareness training pro-gram needs to be created in a way that not only expands employees' knowledge but also inspires them to adopt compliant behaviors.

Today, cybersecurity plays a crucial role in defending against hackers and cyber-criminals and safeguarding government data, personal information, intellectual prop-erty, and industrial and commercial information. The amount of technology used is closely correlated with the rise of cybercrime. Protecting information and preventing catastrophic global repercussions are the two main objectives of cybersecurity due to the sharp growth in cyberattacks [18]. The relevance of cybersecurity education and training is growing, yet there is a dearth of systematic studies comparing the efficiency of various cybersecurity education and development approaches. This review seeks to provide a thorough analysis of the current state of cybersecurity awareness and train-ing to better inform the development and implementation of effective cybersecurity training programs for individuals and organizations. The purpose of this critical as-sessment is to assess the advantages and disadvantages of existing cybersecurity awareness frameworks and training approaches. The significance of this study lies in its assessment of established cybersecurity awareness frameworks and training methodologies. The following is the ultimate research question that will be investigated:

- What is the impact of the models utilized to increase cybersecurity awareness through training and awareness?

2. Concepts

Cybersecurity awareness has become a crucial concern for people and companies due to our rising dependence on technology and the rise of cyber threats. Numerous cybersecurity awareness frameworks and training models have been created by re-searchers to solve this topic. These frameworks and models are intended to improve people's and organizations' knowledge and abilities in identifying, avoiding, and responding to cyber threats. The important terms and terminologies about cybersecurity awareness, frameworks, and training methods will be thoroughly reviewed in this part. This section also covers the potential repercussions of cyberattacks and the significance of cybersecurity awareness and training in today's digital society.

2.1. Cybersecurity Awareness

In addition to organizing the resources and processes connected to cyberattacks, cybersecurity also entails protecting cyberspace [19]. The failure to abide by the cyber-security recommendations made by businesses is the main factor contributing to the rise in cyberattacks. Alharbi and Tassaddiq [20] emphasize the importance of implementing and upholding cybersecurity policies throughout all organizational divisions. As the most exposed link in the organization's security chain, they emphasize the importance of concentrating on its members. This emphasizes how important it is to en-courage solid cybersecurity procedures among employees to strengthen overall organizational security. In the context of online security and privacy, Acquisti et al. [21] also stress the importance of gently encouraging users to make the best decisions possible regarding the sharing of their personal information. People can be helped to make more informed decisions regarding their online safety and data protection by using non-intrusive interventions.

The use of internet-connected intelligent devices has increased as a result of the quick development of technology, particularly in the field of education. In 2020, there will be more than 4 billion smart gadgets, which will intensify cyberattacks and pro-vide new difficulties [22]. To reduce the risk of data security that results from human-related vulnerabilities, cybersecurity awareness is crucial to decrease the risk of human vulnerability [23]. One study's objective is to halt any assaults that aim to exploit human factors in the data security chain. Recognizing and mastering the relevance of data security in terms of individuals should be one of the main and long-term goals of an organization's information security policy [24]. The key components of the industry are, nevertheless, given more focus in the industrial setting. All facets of industrial cyber security awareness receive scant attention. To develop cyber security incident response systems, security awareness is crucial.

Despite being generally well-prepared, cyber security protection systems cannot eliminate network security flaws. This is closely related to the fact that human error continues to be the weakest link in the cyber security chain [25]. The research by Hadlington and Parsons [26] demonstrates how many workers frequently disregard cybersecurity technology. Major security incidents may arise as a result of human mistakes within the company, either directly or indirectly. As a result, it's critical to safe-guard information security against bad information security practices at the individual level [27]. To understand how many elements like cyber security perception, prior cyber security breaches, knowledge, and IT usage may collectively or individually affect cyber security behavior, Kovačević et al. [28] conducted a thorough analysis of cyber security awareness. Organizations should employ frequent training as a way to increase cyber security awareness to prevent or lessen the impact of cyber assaults on business performance [12]. Enhancing security experts' knowledge of current risks and degree of expertise, as well as raising public and non-security professional awareness of cybersecurity, are two ways that cybersecurity training can be provided [29]. Through practice and frequent implementation of better-managed cyber security knowledge, employees can acquire the cyber security skills needed to handle and respond to cyber security risks and dangers [13].

Despite initiatives to raise information security knowledge, little is known about efficient ways to spread that awareness. To do this, Abawajy [23] concentrated on identifying the security awareness delivery strategy that promotes information security awareness. Their main goal was to provide a framework for cyber security education and awareness that would help all internet users develop a culture of online safety [30]. An ideal program would provide a larger portion of its budget to employee training that would prepare them to handle security threats at lower security levels and mitigate more losses at higher security levels [31]. Industrial control systems must establish a

culture of cybersecurity awareness to positively influence employees' cyber security behavior and ultimately enhance the organization's ability to deal with cyber security threats [32].

2.2. Cybersecurity Awareness Frameworks

The cybersecurity framework is the framework that a company needs in order to protect itself from cyberattacks [33]. In today's data-driven digital economy, cyber-crime threats have posed enormous hurdles for enterprises [34]. Managers and policymakers have been forced to reevaluate cybersecurity measures at the individual, organizational, sectoral, and national levels as a result of the severity of the problem [35, 36]. Human factors have recently received substantial attention; technology still plays a crucial part in addressing cybersecurity challenges [37]. Scholars and practitioners have specifically underlined the significance of specialist cybersecurity training, education, and expertise for individual employees, along with essential managerial competencies and infrastructure. In the contemporary data-driven corporate environment, these factors are viewed as being the most crucial for fostering cybersecurity awareness both within and outside organizational borders [38, 39].

By creating and implementing security controls and procedures, an organization's primary goal of cybersecurity is to safeguard its information and data systems from cybercrimes [40]. Cybercrime is the deliberate attempt to endanger a company's valuable assets by making a concerted effort to compromise the infrastructure of the company [37]. A group of attackers or a lone attacker looks for potential weaknesses in a target organization [41]. An organization may be exposed and rendered vulnerable to cybercrimes due to a lack of a strong and secure technological infrastructure, deficiencies in the cybersecurity experience and knowledge of key personnel, a lack of employee education regarding cybersecurity protocols and compliance, individual-level behavioral issues, or human error [40]. Maalem Lahcen et al. [37] provided insight into the interdisciplinary framework connected to human factors, behavioral, and decision-making techniques in cybersecurity based on a literature study of cybercrime trends and size. They conclude that cybersecurity issues cannot be solved by technology alone.

Organizations can develop a structured and thorough approach to cybersecurity awareness training by using a framework. This approach can cover a wide range of topics, such as the best practices for password management, spotting and avoiding phishing scams, safeguarding sensitive information, and handling security incidents. This method offers a consistent approach to training and assists firms in making sure that all employees, regardless of job function or level of technical skill, receive the same training. Additionally, by utilizing frameworks for cybersecurity awareness, businesses can gauge the success of their training initiatives using indicators like employee feed-back, the frequency of security awareness training, and the volume of security incidents reported.

Organizations may drastically lower the risk of cyberattacks and safeguard their sensitive data and systems by adopting an organized approach to cybersecurity awareness. To create training programs that are effective and address the particular needs and vulnerabilities of an organization, it is imperative to use cybersecurity awareness frameworks. This will help to ensure that all staff members have a basic understanding of cybersecurity and know how to recognize and report potential security incidents. Depending on the particular objective of the awareness campaign, there are numerous cybersecurity awareness subcategories. Table 1 shows some potential subcategories.

Table 1. Description of various cybersecurity awareness subcategories

Cybersecurity awareness subcategories	Description
Phishing awareness	Information about phishing scams, which are frequently used by cybercriminals to deceive users into disclosing personal information, and how to spot and avoid them.
Social engineering awareness	Education on how to spot and avoid social engineering attacks, which is another strategy used by cybercriminals to trick people into exposing sensitive information or taking acts that jeopardize security.
Password hygiene awareness	Instructions on how to avoid password reuse, build strong passwords, and safeguard credentials against theft or breach.
Incident response awareness	Training in identifying security threats, communicating with authorities, and containing any resulting disruption.
Compliance awareness	Data security, privacy, and retention policies and procedures, as well as legal and industry standards, should be taught to employees.

Mobile device security awareness	Instruction on safeguarding portable electronic devices like tablets and smartphones, including topics like password management, data encryption, and app safety.
Network security awareness	Routers, switches, and other network nodes can be better protected with the right training in access control, vulnerability management, and network monitoring.
Cloud security awareness	Training in the best methods for protecting information and applications stored in the cloud, such as those used for encryption, authentication, and data management.
Physical security awareness	Information about the physical device and location security, including monitoring, top access control, and theft prevention techniques.

2.3. Cybersecurity Training Models

The cybersecurity strategy of any firm would be incomplete without cybersecurity awareness training. The program's goal is to instruct workers on how to protect their networks and data against cybercriminals. Cybersecurity awareness training is de-signed to help workers recognize and respond to cyber threats, with the ultimate goal of keeping sensitive company data safe. Continuous training, simulation training, gamified training, computer-based training, and instructor-led training are just a few of the strategies for delivering cybersecurity awareness education. Each model has advantages and disadvantages; businesses need to pick the one that works best for them.

I. Continuous training: Giving staff continuing training all year long as op-posed to just once or twice a year is known as continuous training. Employees need to receive ongoing security awareness training to acquire practical cyber skills they can use at work. Providing ongoing security awareness training can be prevented errors made by the staff as a result of ignorance or ignorance-related mistakes. Additionally, continuous training enables shorter training sessions that keep workers interested.

II. Simulation training: A user can move about, investigate, and interact with a scene while participating in simulation training. Online simulation training is feasible and less expensive than traditional training. It entails developing hypothetical situations that represent actual cyberattacks. With the help of this model, staff members can practice handling a cyberattack in a secure setting without endangering the organization's actual data. Cybersecurity training simulators have already been developed by researchers [42, 43].

III. Gamified training: Gamified training uses gaming aspects to enhance the interaction and engagement of the learning process. Younger employees who could be more open to learning through gaming can benefit the most from this concept. Gamified techniques of training and enhancement can offer an improved cognitive approach for the greater recognition of cybersecurity education and application, enhancing cybersecurity aware-ness for everyday users to practice continuously [44].

IV. Computer-based training: An extensive security education and behavior management program's core element is interactive computer-based training. This concept entails giving employees access to training materials via a computer or mobile device. When compared to instructor-led training, this technique is frequently more affordable and allows for flexible completion times for the employee.

V. Instructor-led training: In this strategy, a live instructor instructs staff members either in-person or via video conferencing. Employees who use this model can ask questions and obtain prompt answers from the teacher.

No matter whatever model a company opts for, it's crucial to make sure the training is interesting, pertinent, and simple to grasp. To make sure that the training program is having the desired effect on employee behavior and lowering the organization's risk of a cyberattack, it is also crucial to frequently assess its success.

3. Research Methodology

A thorough search of the Scopus database was done as part of the literature re-view (April 19, 2023). Keywords used in the search included "cybersecurity aware-ness", "training model", "frameworks", among others that are fully displayed in Table 2.

Table 2. Search of keywords

Title Search	logic gate	Title Search
Cybersecurity awareness	AND	Training model
OR		
Security awareness	AND	Training model
OR		
Cybersecurity awareness	AND	Training
OR		
Cybersecurity awareness	AND	Learning
OR		
Cybersecurity awareness	AND	Education
OR		
Security awareness	AND	Education
OR		
Security awareness	AND	Learning
OR		
Security awareness	AND	Training
OR		
Social engineering awareness	AND	Education
OR		
Social engineering awareness	AND	Learning
OR		
Social engineering awareness	AND	Training
OR		
Phishing awareness	AND	Education
OR		
Phishing awareness	AND	Learning
OR		
Phishing awareness	AND	Training

3.1. Criteria for selecting studies

I. Document and source type should be article and journal, respectively.
II. Articles should propose models or frameworks focusing on cybersecurity awareness
III. Articles with just statistical analysis were removed.
IV. Range of the review is between 2012 and 2022.
V. Articles should be final.

3.2. Selection Process

The 52 primary studies included in this publication were chosen as the main out-put of the critical evaluation undertaken as a result of the method utilized for article selection (Fig. 1).

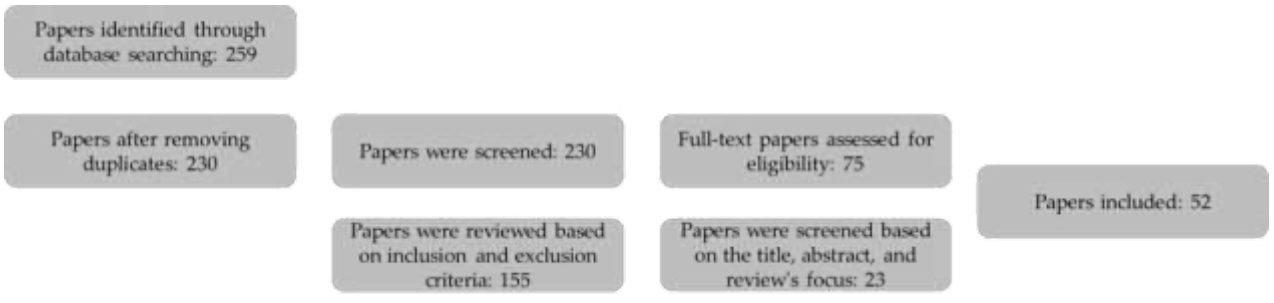

Fig. 1. Flowchart for selecting papers

3.3. Limitations

Especially if a big number of papers need to be analyzed, a thorough literature re-view might take a lot of time. Because of this, potentially relevant studies may be left out of the review. The results of this study may not apply to the broader public since they may not reflect the experiences of all applicable populations or all available evidence. In addition, a restricted database like Scopus was used.

4. Results

This search produced 259 results, of which 207 were removed. This critical evaluation includes 52 publications. Below is a list of the studies that were chosen, along with explanations of the general categorization findings.

Due to the growing relevance of cybersecurity in our increasingly digital society, there has certainly been a growth in the number of papers on cybersecurity awareness frameworks and training models over the years (Fig. 2). The growing prevalence of digital data storage and transmission has made cybersecurity a top priority for individuals, organizations, and governments. This has led to a rise in the importance of and funding for cybersecurity initiatives including education and training programs. It's possible that a combination of circumstances led to 2022 having fewer articles than 2021 did. Researchers may have stopped paying attention to this area of cybersecurity since it's no longer novel. The decline could also be attributable to the fact that the data was collected or made available at a later date.

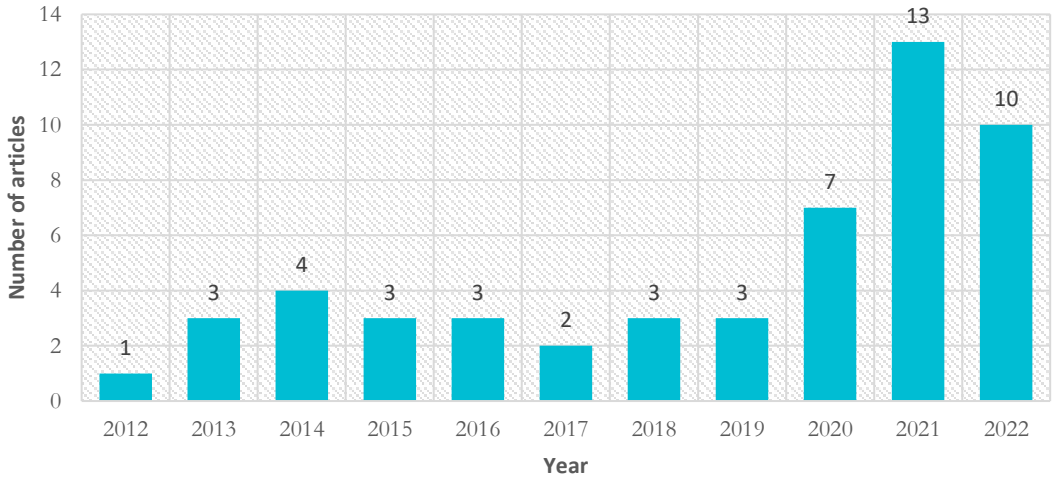

Fig. 2. Number of included papers over the years (2012-2022)

Fig. 3 displays the number of articles organized by subject area. Computer Science (39 papers) is closely related to technology, and cybersecurity is a crucial aspect of defending computer systems and networks against attacks. Therefore, researchers in these disciplines are likely to have a vested interest in developing effective frameworks and training models for cybersecurity awareness. Also applicable to Engineering (19 publications). Social Sciences (19 papers) such as sociology, psychology, and human factors engineering play a crucial role in comprehending how people interact with technology and identifying potential cybersecurity system vulnerabilities. Research in these areas can contribute to the creation of effective frameworks and training models that account for human behavior and social factors.

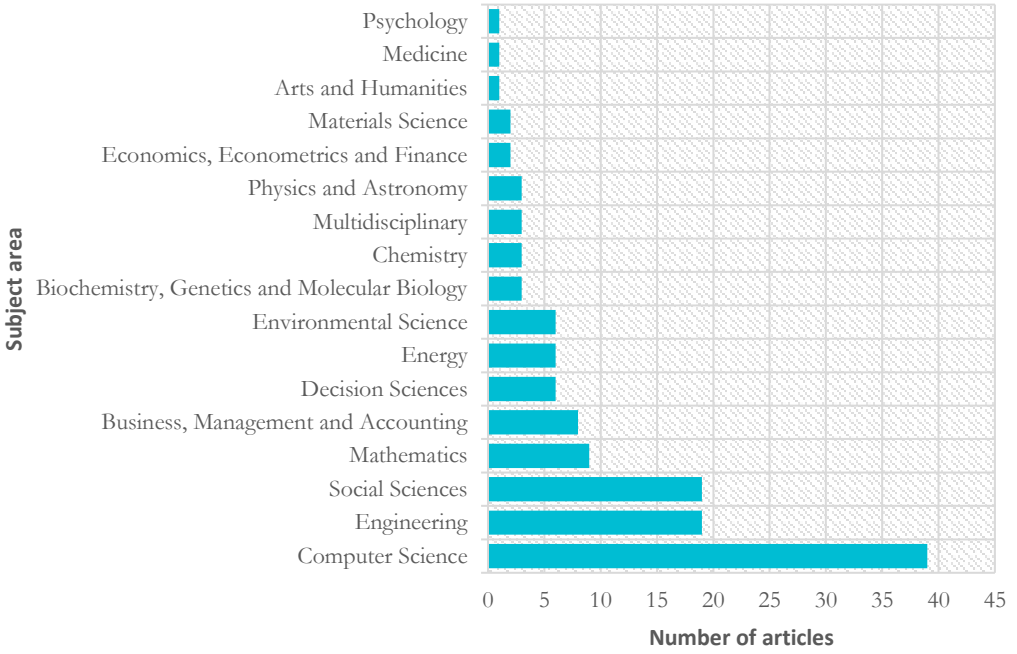

Fig. 3. Number of papers included based on various subject areas

Due to several factors, including China's significant investment in cybersecurity capabilities, population, government policies and regulations protecting citizens and businesses from cyber threats, cultural emphasis on academic achievement and re-search, and overall growth in research output from China, authors from that country have more articles in the field of cybersecurity awareness frameworks and training models. This is shown in Fig. 4. Due to variables such as robust university programs, government involvement in cybersecurity research, and cultural or sociological considerations, authors from Australia and Malaysia may have more work in this area.

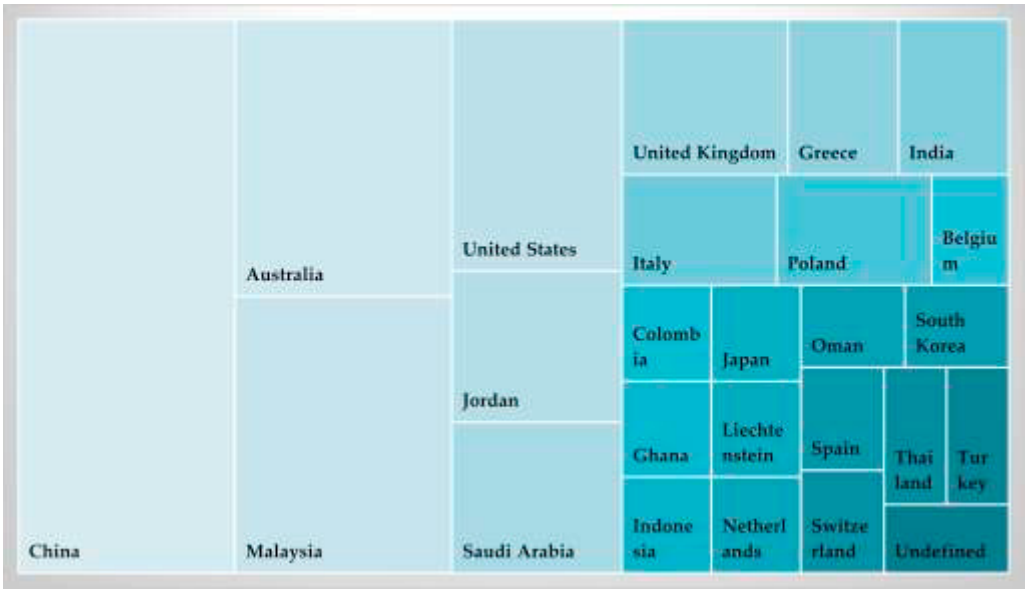

Fig. 4. Contribution of authors from various nations to the articles

The included papers cover a variety of security awareness and education-related topics, particularly in the context of information technology and cybersecurity. Numerous studies emphasize the creation of models for raising awareness and training employees and individuals to better comprehend and respond to security hazards. Phishing, social engineering, network security, and situational awareness are some of the specific areas of concentration.

Several of the studies investigate the use of machine learning and other technologies to enhance security awareness, while others examine the use of serious games or simulations to educate users. Additionally, some studies investigate the efficacy of various training methodologies and the factors that influence the adoption and acceptability of security awareness tools within organizations.

In general, these studies indicate that security awareness is a significant and complex issue that requires ongoing effort. The studies examine a variety of approaches to the problem of enhancing security awareness and emphasize the significance of ongoing education and training in this field. Table 3 displays research concentrations on various cybersecurity awareness techniques.

Table 3. Concentrations of research on different cybersecurity awareness techniques

Cybersecurity awareness techniques	Studies
Cybersecurity awareness training and education	[45-63]
Situational awareness models for cybersecurity	[64-76]
Phishing awareness and prevention	[50, 77, 78]
Social engineering awareness	[45, 79]
Mobile network, and Internet of Things (IoT) security awareness	[62, 80-84]
Energy systems security awareness	[70, 85]
User behavior and awareness	[86-95]

5. Discussion

The goal of this part is to offer a complete review of the benefits and drawbacks of the training methods and cybersecurity awareness frameworks currently in use. The principal inquiry that will be looked into is the following:

- What is the impact of the models utilized to increase cybersecurity awareness through training and awareness?

5.1. Situational Awareness and Cybersecurity

Situational awareness is required for cybersecurity, wireless communication, and IoT systems [64, 67, 69-71, 75, 87]. Numerous researchers have proposed diverse technologies and methodologies while focusing on models and methods for situational awareness in these circumstances. Others provide more generic models for situational awareness in cybersecurity [51, 66, 68, 70], whereas some models focus on specific aspects of situational awareness, such as risk management or evaluation [65, 71-73, 95]. Furthermore, many models include data fusion and machine learning methods to im-prove situational awareness and detect possible threats [51, 65, 66, 69, 72, 87]. Situational awareness models in wireless communication systems are especially significant in emergency scenarios because they can help to ensure that communication remains secure and uninterrupted according to the study by Liang and Gao [87]. To improve situational awareness in wireless sensor networks, Du et al. [95] employ a frequency hopping game model combined with communication security awareness.

Situational awareness is critical for the security of information networks and software chains in the context of IoT systems [65]. Many researchers are researching novel paradigms for situational awareness beyond the classic security perimeter mod-el, in addition to specific technologies and models [67, 69, 75]. Fog and edge computing are emerging as major areas of focus for situational awareness of in-network threats, and new research is being conducted to investigate how these paradigms might be included in situational awareness models [69, 75]. As researchers investigate new technologies and approaches to enhance situational awareness and lower the risk of cyberattacks, the research on situational awareness in cybersecurity, wireless communication, and IoT systems is continually changing.

5.2. Security Awareness Training Models

To defend enterprises against online dangers, security awareness training is essential. Some of the included articles concentrate on various facets of security awareness training, from the employment of cutting-edge techniques to increase training efficacy to the creation of predictive models to customize training materials to specific learn-ers. Using connected open data datasets, Cao et al. [88] and Tan et al. [57] present methods for enhancing security awareness in 5G networks and, respectively, for customizing training content to individual learners. These studies place a strong emphasis on the requirement for practical instruction that covers particular security dangers and difficulties.

Hart et al. [58] describe Riskio, as a serious game that employs gamification to improve cybersecurity education and awareness. A model for adapting security awareness training to individual learning styles is presented in the study by Pattinson et al. [59]. Sabillon [48] and Stefaniuk [46] introduce the CATRAM cybersecurity awareness training paradigm and models for influencing employee information security awareness through training, respectively. These studies stress the significance of creating training programs that enhance employee behavior and safeguard businesses from online threats. For improved resistance to spear phishing attempts and to provide a cybersecurity awareness and training framework for employees who operate re-motely, Caputo et al. [50] and Hijji and Alam [52] suggest concepts for embedded training and awareness. These studies emphasize how crucial it is to offer specialized training that addresses particular security issues. The requirement for security aware-ness training among students is emphasized in the study by Raju et al. [86], which investigates the degree of cybersecurity awareness among students in a higher education setting. In the study by Sutter et al. [77], the usefulness of phishing awareness training is examined, and the necessity of creating predictive models to increase training efficacy is emphasized.

Using a behavioral change paradigm and measuring the effect of training sessions on employees' knowledge of physical security, Cletus et al. [79] and Sas et al. [53] offer strategies for enhancing social engineering awareness, training, and education. The significance of creating efficient training models and assessing their influence on employee behavior is emphasized in these works. Dahabiyeh [54], Alshaikh and Adamson [45], Back and Guerette [78], and Alshaikh et al. [56] discuss adoption and acceptance factors for computer-based security awareness training tools, offer a model for enhancing staff members' security behavior, assess the efficacy of cybersecurity aware-ness training against phishing attacks, and use social marketing to assess the effectiveness of current security education, training, and awareness initiatives in organizations. These studies emphasize the need of comprehending the variables influencing security awareness training efficacy and establish efficient training models that enhance employee behavior and safeguard enterprises against cyber threats.

5.3. Cybersecurity Education and Awareness Programs

In the current digital era, cybersecurity is a critical concern, and companies need to give priority to education and awareness campaigns to reduce the danger of cyberattacks. The studies' diversity, with each offering a different viewpoint on the problem of cybersecurity awareness, is one of its strong points. Some studies like the study by Buja et al. [96] concentrate on creating cybersecurity awareness models for particular populations, while others, like the study by Bada and Nurse [60] concentrate on creating initiatives for particular industry sectors. Studies in this case, also cover a variety of topics related to cybersecurity awareness, such as encouraging the adoption of cybersecurity awareness, training approaches, and adherence to information security policies.

Some studies, however, lack precision and detail regarding the models and pro-grams being produced or assessed. For instance, Apaydin [49] offers a practical model for conducting cybersecurity awareness training, but it's not obvious what precise components the model is made of. Some works also do not include any empirical data to back up their claims or advice. Another drawback is that some works concentrate on particular groups of people or environments, which may limit their adaptability to other situations. For example, Giannakas et al. [62] aim to create cybersecurity education programs that may be given via mobile devices to kids in grades K–6. Even if it's a useful contribution, it's possible that it will not immediately apply to other populations or contexts.

Despite these drawbacks, the books offer insightful analysis and significant advancements in the realm of cybersecurity education and awareness campaigns. Future studies in this field should concentrate on offering more extensive and precise recommendations together with supporting data from empirical studies. In addition, rather than

concentrating on particular groups or situations, research should attempt to cre-ate models and programs that can be customized for other contexts and populations.

5.4. Security Awareness Models for Network and System Management

To guarantee the security of contemporary technologies, security awareness mod-els for network and system management are essential. A study by Sheila et al. [81], emphasizes the demand for mobile users to be security conscious. This book's merit is that it tackles a relevant and topical issue because more and more people are using mobile devices for both personal and business use. The problem, however, is that it does not address any particular models or tactics for network and system management and instead appears to primarily focus on the user's awareness. In the research by Kahtan et al. [82], the topic of security feature embedding in component-based soft-ware development models is covered. Given that security is a top priority for all soft-ware products, this subject excels because it addresses a crucial topic in software development. However, its survey-based design means that it may not offer a thorough grasp of the models or tactics for network and system management.

Guo and Wang [76] examine the network security scenario model for the electric power sector. The specific setting of the electric power industry, which faces particular security concerns, is the strength of this work. The drawback is that it might not apply to different circumstances or sectors. Gautam and Kumar [83] is concerned with cre-ating a security awareness model specifically for the AI and IoT domains. This work's strength is that it covers a crucial and developing field of technology. The drawback is that it might not apply to other fields, and there might be other models or tactics al-ready in use that can be modified for AI and IoT security awareness. Generally, each work has benefits and weaknesses even though they all offer insights into various facets of security awareness models for network and system management. To get a deeper grasp of the subject and to create models and techniques that can be used in a variety of situations and industries, more research may be required.

5.5. Innovative Security Awareness Models

The complexity and sophistication of cybersecurity threats in the modern era need the creation of novel security awareness training methods. Numerous research have looked into various cutting-edge cybersecurity awareness models to instruct and train people on the most recent risks and how to defend themselves from them. According to the study by Ghazvini and Shukur [97], a serious game for the healthcare sector would provide healthcare staff with an interactive and interesting opportunity to learn about information security awareness. To detect knowledge gaps and provide customized training programs, another study by Yue and Ken [94] examined security and students' awareness of the modular object-oriented dynamic learning environment (MOODLE).

According to a study by Lee and Jeong [93] that aimed to raise awareness of in-formation security, notably ransomware, innovative cybersecurity awareness models also employ simulations. Simulations offer an engaging and accurate way to study and experience the effects of cybersecurity threats. The use of Twitter data to identify specific user traits and anticipate awareness levels, which might guide tailored awareness efforts, has been proposed as another method by Yassein et al. [89] for predicting users' awareness of cybersecurity. Another study by Saridewi and Sari [90] stressed the significance of utilizing technology to improve awareness and training programs by suggesting the implementation of machine learning for the human component of information security awareness. Innovative cybersecurity awareness models can also be used to change employee behavior, as in the study by Li et al. [16] proposal of going from awareness to influence. Instead of just concentrating on awareness, this method highlights the significance of influence and doable ways to modify behavior. Cut-ting-edge cybersecurity awareness models offer distinctive and efficient ways to in-struct and train people on the most recent risks and how to defend themselves from them. These methods can raise public knowledge of cybersecurity issues and aid in re-ducing dangers in the current digital era. Table 4 compares the pros and cons of different cybersecurity awareness approaches, covering situational awareness, training models, education programs, network/system management models, and innovative models.

Table 4. Comparative Analysis of Cybersecurity Awareness Approaches

	Situational Awareness	Security Awareness Training Models	Cybersecurity Education and Awareness Programs	Security Awareness Models for Network and System Management	Innovative Security Awareness Models
Benefits					
Enhances Cybersecurity Awareness	✓	✓	✓	✓	✓
Customizable Content		✓	✓		✓
Gamification for Engagement		✓	✓		✓
Addresses Specific Security Issues		✓	✓		✓
Industry-Specific Focus			✓		✓
Focus on Cutting-Edge Threats		✓	✓	✓	✓
Simulations for Experiential Learning			✓		✓
Utilizes Technology and Machine Learning			✓	✓	✓
Drawbacks					
Lack of Specificity	✓	✓	✓	✓	✓
Limited Adaptability	✓	✓	✓	✓	✓
Lack of Empirical Data	✓	✓	✓	✓	✓
Focus on Specific Groups/Situations	✓	✓	✓	✓	✓

6. Conclusions

Safeguarding data integrity and ensuring its long-term stability is contingent upon robust cybersecurity measures. Organizations must accord the utmost priority to cultivating employee awareness and knowledge in the realm of cybersecurity. It is imperative that the broader public actively supports this endeavor as well, as it does not necessitate highly specialized skills. The implementation of well-defined cybersecurity awareness and training programs can substantially reduce the cost and frequency of security incidents for businesses, fortifying their overall security posture and cyber resilience. While comprehensive research assessing the effectiveness of diverse cybersecurity education approaches remains scarce, the importance of cybersecurity education and training is continually on the rise. This review, spanning the years from 2012 to 2022, aims to provide a comprehensive evaluation of the current state of cybersecurity awareness and training.

The articles under scrutiny encompass a wide spectrum of topics related to security awareness and education, particularly within the context of information technology and cybersecurity. Many studies underscore the development of models aimed at heightening awareness and educating individuals to better discern and respond to security threats. Specific areas of focus include situational awareness, network security, social engineering, and phishing. Furthermore, some investigations explore the utilization of serious games or simulations as educational tools. Additionally, several studies delve into the effectiveness of various training methodologies and the factors influencing the adoption and acceptability of security awareness tools within organizations. In summation, the reviewed studies collectively underscore that security awareness is a pivotal and multifaceted issue necessitating continuous dedication and effort.

References

[1] Aloul, F.A., The need for effective information security awareness. Journal of advances in information technology, 2012. 3(3): p. 176-183.

[2] Jalali, M.S., M. Siegel, and S. Madnick, Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. The Journal of Strategic Information Systems, 2019. 28(1): p. 66-82.

[3] Taherdoost, H., A review on risk management in information systems: Risk policy, control and fraud detection. Electronics, 2021. 10(24): p. 3065.

[4] Zhang-Kennedy, L. and S. Chiasson, A systematic review of multimedia tools for cybersecurity awareness and education. ACM Computing Surveys (CSUR), 2021. 54(1): p. 1-39.

[5] Maurseth, P.B., The effect of the Internet on economic growth: Counter-evidence from cross-country panel data. Economics Letters, 2018. 172: p. 74-77.

[6] Wash, R. and E. Rader. Too much knowledge? security beliefs and protective behaviors among united states internet users. in Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015). 2015.

[7] Wash, R. Folk models of home computer security. in Proceedings of the Sixth Symposium on Usable Privacy and Security. 2010.

[8] Camp, L.J., Mental models of privacy and security. IEEE Technology and society magazine, 2009. 28(3): p. 37-46.

[9] Abd Rahim, N.H., et al., A systematic review of approaches to assessing cybersecurity awareness. Kybernetes, 2015. 44(4): p. 606-622.

[10] Shaw, R.S., et al., The impact of information richness on information security awareness training effectiveness. Computers & Education, 2009. 52(1): p. 92-100.

[11] Giannakas, F., et al., A comprehensive cybersecurity learning platform for elementary education. Information Security Journal: A Global Perspective, 2019. 28(3): p. 81-106.

[12] He, W., et al., Improving employees' intellectual capacity for cybersecurity through evidence-based malware training. Journal of intellectual capital, 2020. 21(2): p. 203-213.

[13] Baets, W.R. and G. Van Der Linden, Virtual corporate universities: A matrix of knowledge and learning for the new digital dawn. Vol. 2. 2003: Springer Science & Business Media.

[14] Disparte, D. and C. Furlow, The best cybersecurity investment you can make is better training. Harvard Business Review, 2017. 5.

[15] Mejia, G., Examining the impact of major security breaches on organizational performance: should investing in cybersecurity be a requirement for companies? 2019, Utica College.

[16] Li, L., et al., Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. International Journal of Information Management, 2019. 45: p. 13-24.

[17] Kweon, E., et al., The utility of information security training and education on cybersecurity incidents: an empirical evidence. Information Systems Frontiers, 2021. 23: p. 361-373.

[18] Kemmerer, R.A. Cybersecurity. in 25th International Conference on Software Engineering, 2003. Proceedings. 2003. IEEE.

[19] Craigen, D., N. Diakun-Thibault, and R. Purse, Defining cybersecurity. Technology Innovation Management Review, 2014. 4(10).

[20] Alharbi, T. and A. Tassaddiq, Assessment of cybersecurity awareness among students of Majmaah University. Big Data and Cognitive Computing, 2021. 5(2): p. 23.

[21] Acquisti, A., et al., Nudges for privacy and security: Understanding and assisting users' choices online. ACM Computing Surveys (CSUR), 2017. 50(3): p. 1-41.

[22] Alzubaidi, A., Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. Heliyon, 2021. 7(1): p. e06016.

[23] Abawajy, J., User preference of cyber security awareness delivery methods. Behaviour & Information Technology, 2014. 33(3): p. 237-248.

[24] Hassanzadeh, M., N. Jahangiri, and B. Brewster, A conceptual framework for information security awareness, assessment, and training, in Emerging Trends in ICT Security. 2014, Elsevier. p. 99-110.

[25] Anwar, M., et al., Gender difference and employees' cybersecurity behaviors. Computers in Human Behavior, 2017. 69: p. 437-443.

[26] Hadlington, L. and K. Parsons, Can cyberloafing and Internet addiction affect organizational information security? Cyberpsychology, Behavior, and Social Networking, 2017. 20(9): p. 567-571.

[27] Khando, K., et al., Enhancing employees information security awareness in private and public organisations: A systematic literature review. Computers & security, 2021. 106: p. 102267.

[28] Kovačević, A., N. Putnik, and O. Tošković, Factors related to cyber security behavior. IEEE Access, 2020. 8: p. 125140-125148.

[29] Yamin, M.M., B. Katt, and V. Gkioulos, Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. Computers & Security, 2020. 88: p. 101636.

[30] Kortjan, N. and R. Von Solms, A conceptual framework for cyber-security awareness and education in SA. South African Computer Journal, 2014. 52(1): p. 29-41.

[31] Zhang, Z., et al., Cybersecurity awareness training programs: a cost–benefit analysis framework. Industrial Management & Data Systems, 2021. 121(3): p. 613-636.

[32] Ansari, M.F., A quantitative study of risk scores and the effectiveness of AI-based Cybersecurity Awareness Training Programs. International Journal of Smart Sensor and Adhoc Network, 2022. 3(3): p. 1.

[33] Taherdoost, H., Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. Electronics, 2022. 11(14): p. 2181.

[34] Rawat, D.B., R. Doku, and M. Garuba, Cybersecurity in big data era: From securing big data to data-driven security. IEEE Transactions on Services Computing, 2019. 14(6): p. 2055-2072.

[35] Al-Shanfari, I., W. Yassin, and R. Abdullah, Identify of factors affecting information security awareness and weight analysis process. International Journal of Engineering and Advanced Technology, 2020. 9(3): p. 534-542.

[36] Schneider, B., et al., A Practical Guideline for Developing a Managerial Information Security Awareness Program. 2020.

[37] Maalem Lahcen, R.A., et al., Review and insight on the behavioral aspects of cybersecurity. Cybersecurity, 2020. 3(1): p. 1-18.

Holdsworth, J. and E. Apeh. An effective immersive cyber security awareness learning platform for businesses in the hospitality sector. in 2017 IEEE 25th International Requirements Engineering Conference Workshops (REW). 2017. IEEE.

Al-Janabi, S. and I. Al-Shourbaji, A study of cyber security awareness in educational environment in the middle east. Journal of Information & Knowledge Management, 2016. 15(01): p. 1650007.

[38] Alqahtani, M.S.A. and E. Erfani, Exploring the relationship between technology adoption and cyber security compliance: A quantitative study of UTAUT2 model. International Journal of Electronic Government Research (IJEGR), 2021. 17(4): p. 40-62.

[39] Bauer, S., E.W. Bernroider, and K. Chudzikowski, Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. computers & security, 2017. 68: p. 145-159.

[40] Wen, Z.A., et al. What. hack: engaging anti-phishing training through a role-playing phishing simulation game. in Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. 2019.

[41] Mehmood, S., et al., Sentiment Analysis in Social Media for Competitive Environment Using Content Analysis. 2022.

[42] Das, S. SoK: a proposal for incorporating accessible gamified cybersecurity awareness training informed by a systematic literature review. in Proceedings of the workshop on usable security and privacy (USEC). 2022.

[43] Alshaikh, M. and B. Adamson, From awareness to influence: toward a model for improving employees' security behaviour. Personal and Ubiquitous Computing, 2021. 25(5): p. 829-841.

[44] Stefaniuk, T., Training in shaping employee information security awareness. Entrepreneurship and Sustainability Issues, 2020. 7(3): p. 1832-1846.

[45] Koohang, A., et al., Building an awareness-centered information security policy compliance model. Industrial Management and Data Systems, 2020. 120(1): p. 231-247.

[46] Sabillon, R., et al., An effective cybersecurity training model to support an organizational awareness program: The Cybersecurity Awareness Training Model (CATRAM). A case study in Canada. Journal of Cases on Information Technology, 2019. 21(3): p. 26-39.

[47] Apaydin, F., A practıcal model for informatıon securıty awareness traınıng: Secure informatıon project. Turkish Online Journal of Educational Technology, 2015. 2015: p. 40-45.

[48] Caputo, D.D., et al., Going spear phishing: Exploring embedded training and awareness. IEEE Security and Privacy, 2014. 12(1): p. 28-38.

[49] Liu, X., et al., Network security situation awareness model based on multi-source fusion. Advanced Science Letters, 2012. 5(2): p. 775-779.

[50] Hijji, M. and G. Alam, Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees. Sensors, 2022. 22(22).

[51] Sas, M., et al., The impact of training sessions on physical security awareness: Measuring employees' knowledge, attitude and self-reported behaviour. Safety Science, 2021. 144.

[52] Dahabiyeh, L., Factors affecting organizational adoption and acceptance of computer-based security awareness training tools. Information and Computer Security, 2021. 29(5): p. 836-849.

[53] Al-Shanfari, I., et al., Introducing a novel integrated model for the adoption of information security awareness through control, prediction, motivation, and deterrence factors: A pilot study. Journal of Theoretical and Applied Information Technology, 2021. 99(12): p. 2991-3003.

[54] Alshaikh, M., S.B. Maynard, and A. Ahmad, Applying social marketing to evaluate current security education training and awareness programs in organisations. Computers and Security, 2021. 100.

[55] Tan, Z., et al., Adaptive security awareness training using linked open data datasets. Education and Information Technologies, 2020. 25(6): p. 5235-5259.

[56] Hart, S., et al., Riskio: A Serious Game for Cyber Security Awareness and Education. Computers and Security, 2020. 95.

[57] Pattinson, M., et al., Matching training to individual learning styles improves information security awareness. Information and Computer Security, 2020. 28(1): p. 1-14.

[58] Bada, M. and J.R.C. Nurse, Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). Information and Computer Security, 2019. 27(3): p. 393-410.

[59] Tschakert, K.F. and S. Ngamsuriyaroj, Effectiveness of and user preferences for security awareness training methodologies. Heliyon, 2019. 5(6).

[60] Giannakas, F., et al., Security education and awareness for K-6 going mobile. International Journal of Interactive Mobile Technologies, 2016. 10(2): p. 41-48.

[61] Maqousi, A., et al., A reference model of security requirements for early identification and measurement of security awareness program. Journal of Theoretical and Applied Information Technology, 2014. 63(1): p. 74-84.

[62] Zhao, D., Y. Wu, and H. Zhang, A Situation Awareness Approach for Network Security Using the Fusion Model. Mobile Information Systems, 2022. 2022.

[63] Zhu, X. and H. Deng, A Security Situation Awareness Approach for IoT Software Chain Based on Markov Game Model. International Journal of Interactive Multimedia and Artificial Intelligence, 2022. 7(5): p. 59-65.

[64] Meng, L., Internet of Things Information Network Security Situational Awareness Based on Machine Learning Algorithms. Mobile Information Systems, 2022. 2022.

[65] Qian, M., Evaluation and Prediction Method of System Security Situational Awareness Index Based on HMM Model. Scientific Programming, 2022. 2022.

[66] Nikoloudakis, Y., et al., Towards a machine learning based situational awareness framework for cybersecurity: An SDN implementation. Sensors, 2021. 21(14).

[67] Zhang, H., C. Kang, and Y. Xiao, Research on network security situation awareness based on the lstm-dt model. Sensors, 2021. 21(14).

[68] Chen, H., et al., Situation awareness and security risk mitigation for integrated energy systems with the inclusion of power-to-gas model. IET Renewable Power Generation, 2020. 14(17): p. 3327-3335.

[69] Anjaria, K. and A. Mishra, Relating Wiener's cybernetics aspects and a situation awareness model implementation for information security risk management. Kybernetes, 2018. 47(1): p. 58-79.

[70] Guo, F., et al., A hierarchical P2P model and a data fusion method for network security situation awareness system. Wuhan University Journal of Natural Sciences, 2016. 21(2): p. 126-132.

[71] 7Webb, J., et al., A situation awareness model for information security risk management. Computers and Security, 2014. 44: p. 1-15.

[72] Xu, L., et al., Changes of public environmental awareness in response to the Taihu blue-green algae bloom incident in China. Environment, Development and Sustainability, 2013. 15(5): p. 1281-1302.

[73] Rapuzzi, R. and M. Repetto, Building situational awareness for network threats in fog/edge computing: Emerging paradigms beyond the security perimeter model. Future Generation Computer Systems, 2018. 85: p. 235-249.

[74] Guo, X. and H. Wang, Research on the network security situation awareness model for the electric power industry internal and boundary network. Journal of Applied Sciences, 2013. 13(16): p. 3285-3289.

[75] Sutter, T., et al., Avoiding the Hook: Influential Factors of Phishing Awareness Training on Click-Rates and a Data-Driven Approach to Predict Email Difficulty Perception. IEEE Access, 2022. 10: p. 100540-100565.

[76] Back, S. and R.T. Guerette, Cyber Place Management and Crime Prevention: The Effectiveness of Cybersecurity Awareness Training Against Phishing Attacks. Journal of Contemporary Criminal Justice, 2021. 37(3): p. 427-451.

[77] Cletus, A., B. Weyory, and A. Opoku, Improving Social Engineering Awareness, Training and Education (SEATE) using a Behavioral Change Model. International Journal of Advanced Computer Science and Applications, 2022. 13(5): p. 606-613.

[78] Breitinger, F., R. Tully-Doyle, and C. Hassenfeldt, A survey on smartphone user's security choices, awareness and education. Computers and Security, 2020. 88.

[79] Sheila, M., M.A. Faizal, and S. Shahrin, Dimension of mobile security model: Mobile user security threats and awareness. International Journal of Mobile Learning and Organisation, 2015. 9(1): p. 66-85.

[80] Kahtan, H., N.A. Bakar, and R. Nordin, Awareness of embedding security features into component-based software development model: A survey. Journal of Computer Science, 2014. 10(8): p. 1411-1417.

[81] Gautam, K.K.S. and R. Kumar, Security Awareness Model for Artificial Intelligence and Internet of Things. International Journal on Recent and Innovation Trends in Computing and Communication, 2022. 10(12): p. 203-210.

[82] Lei, W., et al., New Security State Awareness Model for IoT Devices with Edge Intelligence. IEEE Access, 2021. 9: p. 69756-69765.

[83] Zhang, X., H. Zhang, and H. Jiao, Reflections on college students' energy security awareness education in the new era of innovation research and analysis. Open Cybernetics and Systemics Journal, 2015. 9: p. 2582-2586.

[84] Raju, R., N.H.A. Rahman, and A. Ahmad, Cyber Security Awareness In Using Digital Platforms Among Students In A Higher Learning Institution. Asian Journal of University Education, 2022. 18(3): p. 756-766.

[85] Liang, Y. and N. Gao, A Data Symmetry Algorithm-Based Security Awareness Model for Emergency Wireless Communication under Multisensor Fusion. Mobile Information Systems, 2022. 2022.

[86] Cao, H., et al., Embedding Security Awareness for Virtual Resource Allocation in 5G Hetnets Using Reinforcement Learning. IEEE Communications Standards Magazine, 2021. 5(2): p. 20-27.

[87] Yassein, M.M.B., M. Shatnawi, and O.O. Alomari, Users Awareness Prediction of Cyber Security Aspects in Twitter Using Machine Learning Algorithms. International Journal on Communications Antenna and Propagation, 2021. 11(6): p. 383-392.

[88] Saridewi, V.S. and R.F. Sari, IMPLEMENTATION of MACHINE LEARNING for HUMAN ASPECT in INFORMATION SECURITY AWARENESS. Journal of Applied Engineering Science, 2021. 19(4): p. 1126-1142.

[89] Yoo, C.W., G.L. Sanders, and R.P. Cerveny, Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance. Decision Support Systems, 2018. 108: p. 107-118.

[90] Wan Manan, W.N.S., et al., Securing E-learning environment: A study of security awareness and behavior of user. Advanced Science Letters, 2017. 23(11): p. 11272-11275.

[91] Lee, J.H. and J. Jeong, Increase of awareness of the importance of information security using simulation experiment technique model as ransomware. Advanced Science Letters, 2017. 23(10): p. 10246-10249.

[92] Yue, W.S. and L.W. Ken, An exploratory study: Security and students' awareness of modular object-oriented dynamic learning environment (MOODLE). Advanced Science Letters, 2016. 22(12): p. 4138-4141.

[93] Du, C., et al., FHGM: A Frequency Hopping Game Model with Communication Security Awareness for WSN. International Journal of Security and its Applications, 2013. 7(3): p. 223-234.

[94] Buja, A.G., et al., Development of organization, social and individual cyber security awareness model (Osicsam) for the elderly. International Journal of Advanced Technology and Engineering Exploration, 2021. 8(76): p. 511-519.

[95] Ghazvini, A. and Z. Shukur, A serious game for healthcare industry: Information security awareness training program for Hospital Universiti Kebangsaan Malaysia. International Journal of Advanced Computer Science and Applications, 2018. 9(9): p. 236-245.